IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

JENNIFER CABEZAS, *et al.*,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	Civil Action No. 3:23-CV-2453-N
	§	
MR. COOPER GROUP INC., *et al.*,	§	
	§	
Defendants.	§	

MEMORANDUM OPINION AND ORDER

This Order addresses Defendants Mr. Cooper Group, Inc. and Nationstar Mortgage LLC d/b/a Mr. Cooper's (collectively "Mr. Cooper") Motion to Dismiss the Consolidated Class Action Complaint [78]. First, the Court finds that the plaintiffs have standing to bring the claims. Then, for the reasons below, the Court grants the motion to dismiss as to the breach of express contract, unjust enrichment, invasion of privacy, and breach of confidence claims and denies the motion to dismiss as to the breach of implied contract and negligence claims. The Court defers ruling on the negligence per se and individual state law claims until a ruling on class certification. Additionally, the Court finds moot Plaintiffs' Motion to Strike the Declaration of Aaron Scot Miller in Support of Mr. Cooper's Motion to Dismiss [87].

I. ORIGINS OF THE MOTION

Mr. Cooper is a mortgage loan servicer. Pls.' Am. Compl. ¶ 2 [70].[1] On October 31, 2023, Mr. Cooper was the target of a cybersecurity attack. *Id.* ¶ 366. In that attack, ransomware hackers seized control of Mr. Cooper's network and its customers' data. *Id.* ¶ 389. The personal identifying information ("PII") of more than 14 million customers was exposed. *Id.* ¶ 371. This data included the customers' names, addresses, phone numbers, Social Security numbers, dates of birth, and bank account numbers. *Id.* The cybercriminals demanded a ransom payment in exchange for releasing control of the network back to Mr. Cooper and assurance that any customer data was deleted. *Id.* ¶ 389. Mr. Cooper paid the ransom, and the hackers returned control of the systems to Mr. Cooper and provided assurance that the customers' data was deleted from the hackers' system. *Id.* ¶ 391; Defs.' Mot. 1, 4.

Plaintiffs are a putative class of Mr. Cooper customers and former customers whose PII was accessed during the data breach. Pls.' Am. Compl. ¶ 452. They allege that the hackers likely exfiltrated their data during the breach and retained a copy of the data separate from the data the hackers confirmed was deleted when Mr. Cooper paid the ransom. *Id.* ¶ 393–95. Plaintiffs allege that the exfiltrated data is now on the dark web.[2]

---

[1] For the purposes of this motion, the Court accepts the truth of all well-pleaded facts in the complaint.

[2] "The dark web is an area of the internet accessible only by using an encryption tool. It provides anonymity and privacy online, and perhaps consequently, frequently attracts those with criminal intentions." *United States v. Schultz*, 88 F.4th 1141, 1142 n.1 (5th Cir. 2023) (citing Gareth Owen & Nick Savage, *The Tor Dark Net*, Global Commission on Internet Governance, Paper Series No. 20, 1 (2015)).

Id. ¶¶ 27, 88, 118, 219–20, 236, 311. Plaintiffs bring this suit based on damages suffered from the exposure of their data during and following the cyberattack.

As a result of the cyberattack, Named Plaintiffs allege a series of damages that occurred following the data breach and exposure of their PII: Ross, Siegal, Dale, Robertson, Snider, and Watson all allege that they have received notices that their PII is on the dark web. *Id.* ¶¶ 27, 88, 118, 219–20, 236, 311. Ross also alleges that she had money stolen from her bank account. *Id.* ¶ 26. Pollard, Allen, Garrigo, Williams, Burke, and Lepitak allege fraudulent charges on their credit and debit cards. *Id.* ¶¶ 10, 42, 103, 186, 202, 251. Allen, Hansen, Burke, and Marrone allege that they have all experienced fraudulent attempts to open credit cards or bank accounts in their names. *Id.* ¶¶ 41, 168, 201, 281. Pollard, Allen, Robertson, Lepitak, and Curry allege that they received fraud alerts, unauthorized inquiries, or notices of suspicious activity on their credit reports. *Id.* ¶¶ 10, 42, 219, 251, 341. Burani, Williams, and Josi allege that a bad actor gained access to their bank account, and Snider received alerts about a bad actor attempting to gain access to his bank and PayPal accounts. *Id.* ¶¶ 236, 266, 296, 326. In addition, all Named Plaintiffs allege that they have experienced an increase in spam calls, texts, and/or emails, and that they have spent multiple hours on efforts to react to and protect themselves from the harm resulting from the data breach. *Id.* ¶¶ 11, 12, 27, 28, 43, 44, 58, 59, 73, 74, 88, 89, 103, 104, 118, 119, 135, 136, 153, 154, 169, 170, 186, 187, 204, 205, 221, 222, 236, 237, 251, 252, 266, 267, 281, 282, 296, 297, 312, 326, 327, 341, 342.

Defendants bring this motion to dismiss, arguing first that Plaintiffs lack standing and second that the Court should dismiss each of the twenty-seven claims for failure to state a claim.

II. LEGAL STANDARDS

A. Rule 12(b)(1) Standard

Under the United States Constitution, a federal court may decide only actual "cases" or "controversies." U.S. CONST. art. III, § 2. A court properly dismisses a case where it lacks the constitutional power to decide it. *Home Builders Ass'n of Miss., Inc. v. City of Madison*, 143 F.3d 1006, 1010 (5th Cir. 1998). "The justiciability doctrines of standing, mootness, political question, and ripeness all originate in Article III's 'case' or 'controversy' language." *Choice Inc. of Tex. v. Greenstein*, 691 F.3d 710, 715 (5th Cir. 2012) (quoting *Daimler Chrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006)) (internal quotation marks omitted). "Standing and ripeness are required elements of subject matter jurisdiction and are therefore properly challenged on a Federal Rule of Civil Procedure 12(b)(1) motion to dismiss." *Roman Cath. Diocese of Dallas v. Sebelius*, 927 F. Supp. 2d 406, 415–16 (N.D. Tex. 2013) (citing *Xerox Corp. v. Genmoora Corp.*, 888 F.2d 345, 350 (5th Cir. 1989) and *Western Geco L.L.C. v. Ion Geophysical Corp.*, 776 F. Supp. 2d 342, 350 (S.D. Tex. 2011)).

The standing requirement has three elements: (1) injury in fact, (2) causation, and (3) redressability. *See Bennett v. Spear*, 520 U.S. 154, 167 (1997). The injury cannot be merely "conjectural or hypothetical." *Summers v. Earth Island Inst.*, 555 U.S. 488, 493 (2009). Causation requires that the injury "fairly can be traced to the challenged action of

the defendant" rather than to "the independent action of some third party not before the court." *Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 41–42 (1976). And redressability requires that it is likely, "as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (quoting *Simon*, 426 U.S. at 38, 43). "'[W]hen standing is challenged on the basis of the pleadings,' [courts] must 'accept as true all material allegations of the complaint and . . . construe the complaint in favor of the complaining party.'" *Ass'n of Am. Physicians & Surgeons, Inc. v. Tex. Med. Bd.*, 627 F.3d 547, 550 (5th Cir. 2010) (quoting *Pennell v. City of San Jose*, 485 U.S. 1, 7 (1988)) (first alteration and omission in original).

B. Rule 12(b)(6) Standard

When deciding a Rule 12(b)(6) motion to dismiss, a court must determine whether the plaintiff has asserted a legally sufficient claim for relief. *Blackburn v. City of Marshall*, 42 F.3d 925, 931 (5th Cir. 1995). A viable complaint must include "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). To meet this "facial plausibility" standard, a plaintiff must "plead[] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A court generally accepts well-pleaded facts as true and construes the complaint in the light most favorable to the plaintiff. *Gines v. D.R. Horton, Inc.*, 699 F.3d 812, 816 (5th Cir. 2012). But a plaintiff must provide "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555 (internal citations omitted). "Factual allegations must be enough to raise a right to relief above the

speculative level . . . on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *Id.* (internal citations omitted).

In ruling on a Rule 12(b)(6) motion, a court generally limits its review to the face of the pleadings, accepting as true all well-pleaded facts and viewing them in the light most favorable to the plaintiff. *See Spivey v. Robertson*, 197 F.3d 772, 774 (5th Cir. 1999). However, a court may also consider documents outside of the pleadings if they fall within certain limited categories. First, "[a] court is permitted . . . to rely on 'documents incorporated into the complaint by reference, and matters of which a court may take judicial notice.'" *Dorsey v. Portfolio Equities, Inc.*, 540 F.3d 333, 338 (5th Cir. 2008) (quoting *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007)). Second, "[a] written document that is attached to a complaint as an exhibit is considered part of the complaint and may be considered in a 12(b)(6) dismissal proceeding." *Ferrer v. Chevron Corp.*, 484 F.3d 776, 780 (5th Cir. 2007). Third, a "court may consider documents attached to a motion to dismiss that 'are referred to in the plaintiff's complaint and are central to the plaintiff's claim.'" *Sullivan v. Leor Energy, LLC*, 600 F.3d 542, 546 (5th Cir. 2010) (quoting *Scanlan v. Tex. A&M Univ.*, 343 F.3d 533, 536 (5th Cir. 2003)). Finally, "[i]n deciding a 12(b)(6) motion to dismiss, a court may permissibly refer to matters of public record." *Cinel v. Connick*, 15 F.3d 1338, 1343 n.6 (5th Cir. 1994) (citation omitted); *see also, e.g.*, *Funk*, 631 F.3d at 783 (stating, in upholding district court's dismissal pursuant to Rule 12(b)(6), that "[t]he district court took appropriate judicial notice of publicly-available documents and transcripts produced by the [Food and Drug

Administration], which were matters of public record directly relevant to the issue at hand").

III. THE COURT FINDS STANDING

Defendants argue that Plaintiffs lack standing because they failed to plead facts sufficient to allege that they suffered a legally cognizable injury in fact. Defs.' Mot. 5–26. In response, Plaintiffs allege that they have alleged concrete and particularized harms through: (1) misuse of their PII in the form of fraudulent charges and transactions; (2) a post-breach increase in spam calls, texts, and emails; (3) breach of contract; (4) loss of PII value; (5) disclosure of their PII to third parties; (6) expenses associated with prevention, detection, and recovery from exposure of PII and identity theft; (7) opportunity costs associated with mitigating exposure of PII; (8) time, effort, and expense of managing and monitoring accounts in response to the heightened risk from the exposure; (9) anxiety and emotional distress; (10) loss of privacy; (11) loss of benefit of the bargain; (12) imminent risk of harm through fraud or identity theft. Pls.' Resp. 8.

Standing in the data breach context is a fairly nascent area of law and has not yet been comprehensively addressed by the Fifth Circuit or the Supreme Court.

The Fifth Circuit has touched on the issue in *Ellis v. Cargill Meat Solutions*, 2024 WL 4692024 (5th Cir. 2024) (unpub.). There, the court upheld the district court's dismissal of the plaintiff's privacy claims against his employer for lack of standing. *Id.* at *3. The court found that his injuries were too speculative because he made "no allegation that any hacker, identity thief, or third party accessed his data." *Id.* The plaintiff in that case alleged, among a number of other claims against his former employer, that a ransomware

attack against a software company used by the employer had the potential to expose his data. *Id.* at *1. The facts of that case are dissimilar to the pleadings here, where the Plaintiffs here have alleged facts to show that the ransomware attack actually targeted their PII, that their PII was exposed to the hackers for the duration of the attack, and that their exposed PII was published on the dark web.

Because of the factual and pleading dissimilarities to that case, the Court therefore looks to persuasive guidance, first of other circuit courts that have addressed this issue, then at the decisions of other district courts in the Fifth Circuit.

A. The Second Circuit's Factor Test

The First, Second, and Third Circuits use a factor test established by the Second Circuit in *McMorris v. Carlos Lopez & Associates.*, 995 F.3d 295 (2d Cir. 2021), adopted by the Third Circuit in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022), and used by the First Circuit in *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365 (1st Cir. 2023). The test looks at three non-exhaustive factors as guideposts for the court to determine whether an injury is sufficiently imminent for the purposes of standing. *Clemens*, 48 F.4th at 153. The test analyzes:

> (1) Whether the data at issue was compromised "as the result of a targeted attack intended to obtain the plaintiffs' data";
>
> (2) Whether "at least some part of the compromised dataset has been misused — even if plaintiffs' *particular* data . . . has not yet been affected"; and
>
> (3) Whether the data at issue "is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed."

McMorris, 995 F.3d at 301–02. The test does not require fulfillment of each factor, but rather uses these, along with other relevant factors, as guidance to show whether the

plaintiff has shown an injury in fact sufficient for standing. *Id.* ("These factors are by no means the only ones relevant . . . [a]fter all, determining standing is an inherently fact-specific inquiry."); *see also Clemens*, 48 F.4th at 154 ("Of note, misuse is not necessarily required.").

The Second Circuit, building on the cases following *McMorris*, has also found that exposure of PII "as the result of a targeted attempt by a third party to access the data set" is sufficient to show a concrete and imminent injury for the purposes of standing. *Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 288–89 (2d Cir. 2023). The court in that case compared an exposure of PII by data breach to the Supreme Court's ruling in *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), where the Supreme Court "recognized that 'disclosure of private information' was an intangible harm 'traditionally recognized as providing a basis for lawsuits in American courts.'" *Bohnak*, 79 F.4th at 286 (quoting *TransUnion*, 594 U.S. at 425).

The Eleventh Circuit also relies on *TransUnion* to add the caveat that "mere risk of future harm, without more, does not give rise to Article III standing for recovery of damages, even if it might give rise to Article III standing for purposes of injunctive relief." *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023). However, that court found standing where plaintiffs' pleading extended beyond mere risk of harm and alleged that their credit card and personal information was "exposed for theft and sale on the dark web." *Id.*

While other circuits have addressed standing in data breach cases,[3] the relevant decisions pre-date the Supreme Court's analysis in *TransUnion*. Therefore, the Court finds the persuasive power of those cases is diminished by the intervening ruling and does not examine them in more depth here.

B. Decisions of District Courts in the Fifth Circuit

Cases from other district courts in the Fifth Circuit are also persuasive. Courts in the Eastern District of Texas, Western District of Texas, and Western District of Louisiana have adopted the *McMorris* factor test. In the Western District of Texas, in *Hays v. Frost & Sullivan, Inc.*, 2024 WL 4052741 (W.D. Tex. 2024), the court used the *McMorris* factor test and found "a concrete Article III injury to support [the plaintiff's] claim for damages based on the actual and imminent risk of future identity theft and the separate harm caused by that risk, namely the expenditure of time and money enrolling in credit monitoring services." *Id.* at *7. The court also found that the plaintiff's allegation that his PII was published on the dark web was "itself a concrete injury sufficient to confer standing to pursue damages in a data breach case." *Id.*

In the Eastern District of Texas, in *Smith v. American Pain and Wellness, PLLC*, 747 F. Supp. 3d 989 (E.D. Tex. 2024), the court examined the holdings of *Bohnak*, *Webb*,

[3] For a more detailed discussion of rulings from other circuits, see *Hulse v. Acadian Ambulance Service Inc.*, 2025 WL 1453847, at *5–6 (W.D. La. 2025) (citing cases from the Fourth, Sixth, Seventh, Eighth Ninth, and D.C. Circuits, which all predate the Supreme Court's decision in *TransUnion*) and *Williams v. Bienville Orthopaedic Specialists, LLC*, 737 F. Supp. 3d 411, 418 (S.D. Miss. 2024) (discussing the apparent circuit split over the issue prior to *TransUnion* and the rulings predating that decision in the Seventh, Eighth, and Eleventh Circuits).

and *Clemens*, and found them persuasive. *Id.* at 1002. The court in that case held that the plaintiffs established Article III standing when they alleged (1) the exposure of their PII to a third party, (2) the time and money spent mitigating risks of identity theft, and (3) emotional distress based on the data breach causing substantial risks of identity theft. *Id.* at 1002–03.

In the Western District of Louisiana, the court in *Hulse v. Acadian Ambulance Service Inc.*, 2025 WL 1453847 (W.D. La. 2025), also adopted the Second Circuit's *McMorris* factor test. *Id.* at *6. That court held that "publication of one's personal information on the dark web constitutes a present injury." *Id.* at *7. The court in *Castillo v. Berry Bros General Contractors Inc.*, 2025 WL 1062091 (W.D. La. 2025) also followed the *McMorris* test and found standing because the plaintiff's first and last name and Social Security number were exposed in a data breach where an unauthorized party obtained files containing the PII. *Id.* at *1, 3.

Additionally, courts in the Eastern District of Texas and Southern District of Mississippi have found the holdings from *Bohnak* persuasive. The *Smith* court in the Eastern District of Texas followed *Bohnak*'s analysis of *TransUnion* and concluded "an injury arising from [disclosure of private information] is concrete for the purposes of Article III standing." *Smith*, 747 F. Supp. 3d at 1001. And in the Southern District of Mississippi, the court in *Williams v. Bienville Orthopaedic Specialists, LLC*, 737 F. Supp. 3d 411 (S.D. Miss. 2024), also adopted the Second Circuit's reasoning in *Bohnok*. *Id.* at 419–421. That court found standing for plaintiffs who alleged actual misuse of their data, but not for plaintiffs who alleged only an increase in spam communications or for

mitigation efforts without a showing of "alleged misuse or actual access." *Id.* at 421–22; *see also id.* at 421 (citing *Green-Cooper*, 73 F.4th at 889, for the holding that "allegations that personal information was exposed for theft and sale on the dark web is sufficient to establish an injury in fact.").

Finally, in the Southern District of Texas, two courts have found no standing in a data breach context where the pleadings did not sufficiently allege that the plaintiffs' PII had been misused. The court in *Perlacki v. J.B. Poindexter & Co., Inc.*, 2025 WL 754503 (S.D. Tex. 2025), did not find standing because the court found there that the heightened risk of identity theft and fraud was not a concrete injury because the plaintiff did "not allege that his PII has been sold on the dark web or to a criminal enterprise [or] that any of his PII has actually been misused." *Id.* at *3. Similarly, in *Logan v. Marker Group, Inc.*, 2024 WL 3489208 (S.D. Tex. 2024), the court found no standing where the plaintiffs had failed to allege that they were victims of actual identity theft, and thus the court determined that the risk of future harm was entirely speculative. *Id.* at *6. There, the court held that the plaintiffs did not plausibly allege causation because they failed to plausibly suggest that the misuse of PII was a result of the breach. *Id.* at *5.

C. The Court Finds Plaintiffs Have Sufficiently Alleged an Injury in Fact

1. Spam communications do not constitute an injury in fact. — First, each of the Plaintiffs have alleged an increase in spam calls, texts, and/or emails following the data breach. Courts have found that an "allegation of an increase in spam phone calls is insufficient to establish an injury in fact." *Williams*, 737 F. Supp. 3d at 421; *see also McCombs v. Delta Grp. Elec., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023) ("Spam

calls, texts, and e-mails have become very common in this digitized world, and a number of courts have declined to confer standing when considering an increase in spam communications.") (collecting cases); *Perlacki*, 2025 WL 754503, at *4 ("[S]pam is not a concrete harm."). The Court agrees with these rulings that spam communications alone are not enough to establish injury in fact.

2. Plaintiffs have not established standing under theories of diminution of value or loss of benefit of the bargain. — The Court also finds that the Plaintiffs' claims of injury-in-fact based on a diminution in value of their PII and a lack of benefit of the bargain are not persuasive. "Courts are divided on whether diminution of value of personal information constitutes a concrete harm." *Hulse*, 2025 WL 1453847, at *8. But "district courts in Texas are more skeptical" than many other courts as to a diminution of value for PII claim. *In re ESO Sols., Inc. Breach Litig.*, 2024 WL 4456703, at *7 (W.D. Tex. 2024).

Even if the Court found diminution of value a concrete harm, because Plaintiffs fail to allege that they intended or attempted to sell their data and were forced to do so at a diminished price, the Court finds that they have not plausibly pled diminution of value. *See In re ESO*, 2024 WL 4456703, at *7 (rejecting diminution of value claims because "[e]ven if diminished PII was cognizable in the Fifth Circuit, Plaintiffs do not plausibly show their PII has diminished in value. Plaintiffs fail to allege that they attempted to or would have ever sold their PII."); *Williams*, 737 F. Supp. 3d at 422 (rejecting the same because "[t]here is no allegation that any of the plaintiffs . . . intended to sell their private information.").

Likewise, Plaintiffs fail to plead a loss of benefit of the bargain because they have failed to adequately plead that they bargained for and paid for the protection of their private information. *See Williams*, 737 F. Supp. 3d at 422 ("There is no allegation that any of the plaintiffs paid a certain amount of money to [the company] in exchange for protection of their private information."). At most, Plaintiffs have alleged that Mr. Cooper's Privacy Policy stated that the company used security measures to protect customers' personal information. Pls.' Am. Compl. ¶ 465. Benefit of the bargain theories for standing are disfavored in the data breach context. *See, e.g.*, *Podroykin v. Am. Armed Forces Mut. Aid Ass'n*, 634 F. Supp. 3d 265, 272 (E.D. Va. 2022); *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 695 (7th Cir. 2015) (describing benefit of the bargain theories in this context as "dubious"); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 995 (W.D. Okla. 2021). "And even courts willing to entertain this theory of standing consistently reject this theory in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach." *Podroykin*, 634 F. Supp. 3d at 272 (cleaned up). The Court finds that Plaintiffs have not sufficiently alleged either that data protection was part of the bargain for services with Mr. Cooper, or that they have lost any of services they bargained for under their contract with Mr. Cooper.

Therefore, the Court finds both these theories unavailing.

3. The Court finds Plaintiffs have sufficiently alleged an increased risk of future harm. — Next, the Court follows the persuasive authority discussed above and adopts the *McMorris* factor test to analyze risk of imminent future harm for standing in the data breach context.

First, the Court finds that the data at issue was clearly compromised "as the result of a targeted attack intended to obtain the plaintiffs' data." *McMorris*, 995 F.3d at 301. The ransom attack used a strategy of exfiltrating customer data in order for the hackers to make a ransom demand for its return. Defs.' Mot. 3–4. In negotiating the ransom demand, Mr. Cooper confirmed with the hackers that "the data they possessed was customer data extracted during the attack, including personally identifiable information." *Id.*

Next, Plaintiffs have sufficiently alleged that "at least some part of the compromised dataset has been misused." *McMorris*, 995 F.3d at 301. A number of Plaintiffs allege that due to the exposure of their data to third parties, they have suffered fraudulent credit card charges, Pls.' Am. Compl. ¶¶ 10, 42, 103, 185, 201–03, 251; unauthorized attempts to access or open bank and credit card accounts in their names, *id.* ¶¶ 42, 168, 201–203, 219, 236, 251, 266, 281, 296; had money stolen from an account, *id.* ¶ 26; had their bank or other financial accounts accessed, *id.* ¶¶ 236, 266, 296, 326; and have received information about their PII being discovered and disseminated on the dark web. *Id.* ¶¶ 27, 88, 118, 220, 236, 311. The Court finds these allegations sufficient to allege that at least some portion of the data was misused.

Finally, the Court finds that the particular data at issue, including Plaintiffs' "names, addresses, phone numbers, Social Security numbers, dates of birth, and bank account

numbers," *id.* ¶ 371, is the type of data that is "likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed." *McMorris*, 995 F.3d at 302. This is precisely the type of data contemplated by the court in *McMorris*. *See id.* ("Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth — especially when accompanied by victims' names — makes it more likely that those victims will be subject to future identity theft.").

Because the Court finds that all three factors weigh toward a finding that Plaintiffs have shown an imminent risk of future harm, the Court finds that all Plaintiffs have standing based on the risk of future harm.

4. Exposure of Plaintiffs' data to a third-party and on the dark web does sufficiently constitute an injury in fact. — Additionally, the Court finds that Plaintiffs have established a present injury in the allegations of the sale or exposure of their PII to the dark web. Each of the Plaintiffs has alleged that his or her "PII was improperly accessed and obtained by unauthorized third parties" through the ransom attack, as confirmed for each Plaintiff by a letter from Mr. Cooper following the attack. Pls.' Am. Compl. ¶¶ 7, 23, 39, 55, 70, 85, 100, 115, 130, 147, 165, 182, 198, 216, 233, 248, 263, 278, 293, 308, 323, 328. Critically, Mr. Cooper's own factual summary illuminates that the cybercriminal attack was targeted to extract the PII of its customers. Defs.' Mot. 4 (explaining that Mr. Cooper confirmed the data the cybercriminals possessed and was holding for ransom "was customer data extracted during the attack, including personally identifiable information"). Furthermore, Plaintiffs have alleged that their PII was exposed and "is now on the dark

web." *Id.* ¶ 638. Six Plaintiffs have alleged that they received notices that their PII was on the dark web following the ransom attack. *Id.* ¶¶ 27, 88, 118, 220, 236, 311.

The Court finds Plaintiffs have sufficiently alleged that their PII was exposed to a third party and on the dark web. Therefore, following the theory of the Second Circuit in *Bohnok*, based on the Supreme Court's ruling in *TransUnion*, the Court finds that Plaintiffs also have standing based on the exposure of data to an unauthorized third party, similar to a claim for public disclosure of private facts.

5. Because the Court has found a concrete injury, the Court finds standing for mitigation costs and emotional distress. — As other courts have found, mitigation costs cannot themselves create standing. *See Logan*, 2024 WL 3489208, at *6 (finding that the court's determination "that the risk of future identity theft based on the data breach is not a concrete injury sufficient to confer standing, Plaintiffs' . . . harms based on fear of that hypothetical future harm is also insufficient to establish standing."); *Perlaki*, 2025 WL 754503, at *4 ("To establish standing, [plaintiff's] lost time claim must bear a close relationship to some cognizable harm."). However, where courts have already established a risk of future harm, emotional distress and mitigation costs, "when coupled with the risk of harm . . . is a concrete injury sufficient to confer standing." *Hulse*, 2024 WL 1453847, at *8.

6. The Court denies standing for the injunctive relief sought by Plaintiffs because it is based on a speculative future harm not sufficiently imminent or substantial to be a concrete harm. — Finally, for the injunctive relief claim, Plaintiffs plead that "Mr.

Cooper's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security" and do not "employ adequate security practices consistent with law and industry standards" and ask the Court to enjoin Mr. Cooper to remedy the deficient security measures in order to protect customers' data from further attacks. Pls.' Am. Compl. ¶¶ 542, 551. While Plaintiffs have pled that Mr. Cooper retains their data and are able to identify security measures that could be improved, this claim for injunctive relief is based entirely on the speculative risk of a second data breach.

Courts have found that the future harm of a second cyberattack is too speculative and not sufficiently imminent. *See Williams*, 737 F. Supp. 3d at 426 ("Plaintiffs do not have standing to seek declaratory or injunctive relief because they have failed to allege facts 'tending to show that a second data breach is currently impending or there is a substantial risk that one will occur") (quoting *Hummel v. Teijin Auto. Techs., Inc.*, WL 6149050, at *14 (E.D. Mich. 2023)); *Hulse*, 2025 WL 1453847, at *9 (discussing the Third Circuit's holding of the same and concluding that "Plaintiffs lack standing to seek injunctive relief based on the prospect of future cyberattacks"). The Court therefore finds that Plaintiffs lack standing to seek injunctive relief for the speculative future harm of a second cyberattack.

D. The Court Finds Causation

Because Plaintiffs have sufficiently alleged an injury in fact, the Court turns to whether Plaintiffs have pled sufficient facts to establish that the injury is fairly traceable to the ransom attack. Defendants argue that Plaintiffs have failed to establish a connection because (1) "evidence shows that the cybercriminals deleted the files containing the data

they took from Mr. Cooper"; (2) the Plaintiffs "do not allege any facts demonstrating that Mr. Cooper ever had the PII necessary to engage in unauthorized" credit card and bank account transactions; and (3) Plaintiffs' allegations that the attempts occurred within the nine months after the ransom attack "is hardly sufficient to establish traceability." Defs.' Mot. 6–11.

However, Plaintiffs have sufficiently alleged that Defendants failed to adequately prepare for a cyberattack and secure their PII. Pls.' Am. Compl. ¶¶ 375, 390, 410, 412–32, 451, 470, 536. They have alleged that Mr. Cooper was subject to a ransom attack where Plaintiffs' PII was seized. *Id.* ¶¶ 2, 388–395. This PII included birth dates, bank account numbers, and social security numbers. Pls.' Am. Compl. ¶¶ 2, 371, 378. Plaintiffs also allege this is exactly the PII identity thieves use for crimes including credit card, bank, and finance fraud. *Id.* ¶¶ 437–38, 446.

The heightened factual pleading standard that Defendants attempt to impose is procedurally premature. Courts have found that "the plaintiff's burden is 'relatively modest' at the pleading stage of the litigation." *Williams*, 737 F. Supp. 3d at 423. In data breach cases, the pleading standard for causation can be met where plaintiffs have pled "(1) the defendant failed to secure his private information; (2) its network was subsequently hacked; (3) the plaintiff's private information was stolen by hackers; and (4) the plaintiff became the victim of [the pled injury in fact]." *Id.*; *see also Merrell v. 1st Lake Props., Inc.*, 2023 WL 6316257, at *4 (E.D. La. 2023) ("Plaintiff has alleged that he does not recall receiving any other notices of data breach, and that his PII was compromised because

defendant failed to implement minimum safeguards. . . . At this stage, nothing further is required to establish traceability for constitutional purposes.").

The Court finds that Plaintiffs have met their pleading standard for causation.

E. The Court Finds Redressability

Defendants argue that Plaintiffs have not sufficiently pled redressability only for the claims regarding injunctive relief. Defs.' Mot. 15. Because the Court has already found that Plaintiffs lack standing for this claim, and Defendants do not otherwise argue that Plaintiffs have not established redressability, the Court finds that all other injuries pled are sufficiently redressable.

IV. THE COURT GRANTS IN PART AND DENIES IN PART THE MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

A. Breach of Contract

Under Texas law, to state a claim for breach of contract, Plaintiffs must allege "(1) the existence of a valid contract; (2) performance or tendered performance by the plaintiff; (3) breach of the contract by the defendant; and (4) damages sustained by the plaintiff as a result of the breach." *Smith Int'l, Inc. v. Egle Grp., LLC*, 490 F.3d 380, 387 (5th Cir. 2007) (quoting *Valero Mktg. & Supply Co. v. Kalama Int'l, L.L.C.*, 51 S.W.3d 345, 351 (Tex. App. — Houston [1st Dist.] 2001, no pet.)). The existence of a valid contract, whether express or implied, requires: "(1) an offer, (2) an acceptance, (3) a meeting of the minds, (4) each party's consent to the terms, and (5) execution and delivery of the contract with the intent that it be mutual and binding." *DeClaire v. G & B McIntosh Fam. Ltd. P'ship*, 260 S.W.3d 34, 44 (Tex. App. — Houston [1st Dist.] 2008, no pet.); *see Univ. Nat'l Bank v. Ernst & Whinney*, 773 S.W.2d 707, 710 (Tex. App. — San Antonio 1989, no writ) ("The

elements of a contract, express or implied, are identical."). In an express contract, the parties usually state and agree to specific terms. *Haws & Gorbett Bros. Welding Co.*, 480 S.W.2d 607, 609 (Tex. 1972). However, an implied contract arises when the parties' acts and conduct create an inference of mutual intention to contract. *Id.*

1. The Court grants the motion to dismiss the breach of express contract claim. — Plaintiffs assert a breach of express contract claim under a theory that Mr. Cooper's Privacy Policy constitutes a contract between Mr. Cooper and its customers, and that Mr. Cooper's failure to protect customers' PII was a violation of that contract. Pls.' Am. Compl. ¶¶ 462–471. Defendants move to dismiss Plaintiffs' breach of contract claim, arguing that the Privacy Policy is a statement of corporate policy, and not, standing alone, an enforceable contract. Defs.' Mot. 28.

Courts that have considered the question of whether a privacy policy may constitute an express contract generally find that it does not. *See Capps v. Bullion Exch., LLC*, 2019 WL 4918682, at *2 (N.D. Okla. 2019) (collecting cases). The Court agrees with Defendants that the general corporate privacy policy appears to be a statement of corporate policy rather than an express contract between Plaintiffs and Defendants. Because Plaintiffs have failed to establish the existence of a valid contract, the Court dismisses the claim for breach of express contract.

2. The Court denies the motion to dismiss the breach of implied contract claim. — Plaintiffs assert a breach of implied contract under the theory that as part of the transactions wherein "Mr. Cooper acquired and maintained the PII of Plaintiffs," Mr. Cooper implicitly agreed to keep that PII safe. Pls.' Am. Compl. ¶¶ 472–81. Plaintiffs claim that implicit in

the transactions to enter into services with Mr. Cooper "was the obligation that Mr. Cooper would utilize reasonable measures to keep the PII secure; Mr. Cooper would limit access to PII; Mr. Cooper would use the PII for approved business purposes only; and Mr. Cooper would retain PII only as necessary to perform necessary business functions." *Id.* ¶ 475. Defendants move to dismiss based upon a lack of implied contract between Plaintiffs and Mr. Cooper, arguing first that the Plaintiffs' contracts were with the mortgage originators, not Mr. Cooper, then that the existence of express contracts governing their mortgage agreement precludes assertion of the existence of an implied contract. Defs.' Mot. 30–31.

Other courts who have addressed similar fact patterns have found that an implied contract is sufficiently alleged where the plaintiffs plead that an implied contract was created by assurance of a privacy policy and in the implied promise to protect and not disclose PII when customers are required to provide PII as a condition of receiving defendant's services. *See, e.g.*, *Hays*, 2024 WL 4052741, at *9–10 (collecting cases); *Hulse*, 2025 WL 1453847, at *13 ("It is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently." (quoting *McFarlane v. Altice, USA, Inc.*, 524 F. Supp. 3d 264, 282 (S.D.N.Y. 2021))).

The Court agrees that Plaintiffs' allegations are sufficient to allege the existence of an implied contract to safeguard the PII. Therefore, the Court denies the motion to dismiss the claim for breach of implied contract.

B. The Court Denies the Motion as to the Negligence Claim

Under Texas law, a negligence claim requires (1) the existence of a duty; (2) a breach of that duty; and (3) damages proximately caused by the breach. *W. Invs., Inc. v. Urena*, 162 S.W.3d 547, 550 (Tex. 2005).

1. Plaintiffs plausibly allege a duty of care. — Defendants argue that Plaintiffs do not sufficiently allege that Mr. Cooper owes Plaintiffs a duty of care because there is no special relationship between a business and its customers to "safeguard collected customer PII from criminal theft." Defs.' Mot. 33. However, unlike the case Defendants cite for that proposition, where the negligence claim was based on the business interaction between the mortgagor and mortgagee, *see Hill v. Lakeview Loan Servicing, LLC*, 2023 WL 3237508, at *1 (N.D. Tex. 2023), Plaintiffs here have alleged that Defendants have a duty to safeguard PII entrusted to them because improperly safeguarding data poses a foreseeable risk that could be avoided by the exercise of ordinary care. *See Mendez v. Caterpillar, Inc.*, 2011 WL 6999659, at *10 (W.D. Tex. 2011) ("A duty arises when a person's conduct poses a foreseeable risk to another that could be avoided by the exercise of ordinary care."). "In determining whether there is a duty, the court considers several factors, including the risk, foreseeability, and the likelihood of injury," weighed against the social utility and cost to the defendant. *Washington v. U.S. Dep't of Hous. and Urban Dev.*, 953 F. Supp. 762, 773 (N.D. Tex. 1996). Plaintiffs argue that the safety of the PII held by Mr. Cooper is out of their direct control, that the risk of a breach is "evident and foreseeable," and that Mr. Cooper's data security was deficient under ordinary standards. Pls.' Am. Compl. ¶¶ 482–489; Pls.' Resp. 30–31. Under this standard, courts have found

that a corporation has a duty to safeguard PII it chooses to retain. *In re ESO*, 2024 WL 4456703, at *9; *see In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 397 (E.D. Va. 2020) (analyzing Texas law and finding that where plaintiffs implemented harmful storage of PII "without adequate safeguards to protect against hacking . . . the Texas Supreme Court would recognize a duty separate and apart from the parties' contractual relationship").[4]

Furthermore, while Defendants argue that a duty of care would not extend to a third-party criminal action, "Texas law recognizes that 'if a criminal's conduct is a foreseeable result of the prior negligence of a party, the criminal act may not excuse that party's liability.'" *In re ESO*, 2024 WL 4456703, at *10 (citing *Barton v. Whataburger, Inc.*, 276 S.W.3d 456, 462 (Tex. App. — Houston [1st Dist.] 2008, pet. denied)). The question turns on whether the plaintiffs plead that (1) the defendant committed negligent acts, and (2) knew or should have known that the crime might occur because of its actions. *Id.* Plaintiffs have sufficiently alleged that Mr. Cooper was negligent in securing Plaintiffs' PII and that, based on Mr. Cooper's own regulatory filings, it is well-aware of the risk of such an attack. Pls.' Am. Compl. ¶¶ 407, 490–91. Defendants further argue that they could not be expected

[4] Defendants cite *Gorman v. Ethos Group Inc.*, 2024 WL 1257493, at *3 (N.D. Tex. 2024), for the quotation that "'no court — let alone a Texas Court or the Fifth Circuit — has recognized a common law duty to safeguard' certain PII." Defs.' Mot. 33 (quoting *Gorman*, 2024 WL 1257493, at *3). That quotation, however, leaves out that the court was referring specifically to driver's license numbers, which the court had found were often publicly available, unsensitive information. The court discussed in that opinion that there might be a common law duty for more sensitive information and gave leave to the plaintiffs there to amend to make arguments about a statutory or common law duty arising from disclosure of plaintiffs' dates of birth.

to safeguard PII from criminal theft because a "duty only exists when the risk of criminal conduct is so great that it is *both* unreasonable and foreseeable." Defs.' Mot. 34–35 (quoting *Jai Jalaram Lodging Grp., L.L.C. v. Leribeus*, 225 S.W.3d 238, 242 (Tex. App. — El Paso 2006, pet. denied)). Defendants argue that in order for the risk to be unreasonable and foreseeable, plaintiffs must show "the defendant being previously and repeatedly exposed to the same criminal activity." *Id.* (citing the same). However, Plaintiffs have alleged that Mr. Cooper's regulatory filings in its 2022 Annual Report state that it is "regularly the subject of attempts by attackers to gain unauthorized access to [its] network, systems, and data, or to obtain, change or destroy confidential data (including personal identifying information of individuals)." Pls.' Am. Compl. ¶ 407. Therefore, because Plaintiffs have clearly pled that Mr. Cooper was previously and repeatedly exposed to the same criminal activity, the Court concludes that plaintiffs have sufficiently pled a high, foreseeable risk that establishes a duty of care.

2. Plaintiffs plausibly allege breach. — Taking Plaintiffs' factual allegations as true, Plaintiffs sufficiently plead a "series of cybersecurity failures and refusal to follow basic cyber hygiene norms." Pls.' Am. Compl. ¶ 374. They allege Mr. Cooper (1) failed to properly encrypt customers' PII, or used "deprecated encryption protocols"; (2) failed to delete PII "after it no longer needed to be retained"; (3) stored PII "in a vulnerable, internet-accessible environment"; (4) failed to use "up-to-date authentication measures"; (5) failed to apply needed software patches "to eliminate known vulnerabilities"; and (6) "failed to monitor traffic on its network . . . to detect malicious activity." *Id.* ¶ 375. The Court finds that this is sufficient to meet the pleading standard for breach.

3. Plaintiffs plausibly allege causation. — Next, Plaintiffs allege that these cybersecurity failures "permitted the cybercriminals to access Mr. Cooper's systems and victimize Class Members." *Id.* ¶ 374. Plaintiffs describe in detail in the complaint how the alleged failures enabled the hackers to gain a foothold into the system[5] and how the alleged deficiencies made the data breach possible. *Id.* ¶¶ 374–395. The Court finds this sufficient at the pleading stage.

4. Plaintiffs plausibly allege damages, and the economic loss rule does not bar Plaintiffs' negligence claim. — Finally, Defendants argue that (1) Plaintiffs fail to plead they suffered damages, and (2) the economic loss rule bars Plaintiffs' negligence claim to the extent that they allege a loss arising from breach of express or implied contract. Defs.' Mot. 37–38. First, as discussed above, Plaintiffs have sufficiently alleged damages.

Next, the economic loss rule does not bar tort claims "when the duty allegedly breached is independent of the contractual undertaking and the harm suffered is not merely the economic loss of a contractual benefit." *Chapman Custom Homes, Inc. v. Dallas Plumbing Co.*, 445 S.W.3d 716, 718 (Tex. 2014). When determining whether an action sounds in tort or contract such that the economic loss doctrine may preclude a particular tort claim, Texas courts "look to the source of the duty allegedly violated and the nature of

[5] Defendants argue that Plaintiffs' allegations regarding Mr. Cooper's cybersecurity measures are irrelevant because some of the allegations of deficiencies predate the attack, for example, that Mr. Cooper's lack of multi-factor authentication in 2022 was irrelevant to the 2023 attack. *See* Defs.' Mot. 36. However, the complaint alleges that the hackers launched an initial attack into the system prior to the attack "likely . . . between 6 months and 2 years prior," Pls.' Am. Compl. ¶ 385, thereby explaining the connection between the alleged deficiency and the attack.

the claimed loss." *El Paso Mktg., LP v. Wolf Hollow I, L.P.*, 383 S.W.3d 138, 143 (Tex. 2012). Here, the Court has determined that the duty to safeguard data does not arise solely out of the contract, and the claimed loss extends beyond the economic losses of the benefits under the contract. Therefore, the Court finds that the economic loss rule does not bar a negligence claim at this stage.

C. The Court Grants the Motion as to the Unjust Enrichment Claim

Plaintiffs assert a claim for unjust enrichment. First, Defendants argue that Texas courts do not recognize unjust enrichment as an independent cause of action. Defs.' Mot. 39. Federal district courts have been inconsistent in their treatment of the issue of unjust enrichment. *Compare Hancock v. Chi. Title Ins. Co.*, 635 F. Supp. 2d 539, 560–61 (N.D. Tex. 2009) (finding Texas courts view unjust enrichment as a general theory of recovery, not a separate cause of action), *with Banion v. Geovera Specialty Ins. Co.*, 2016 WL 7242536, at *3 (S.D. Tex. 2016) ("Texas courts recognize unjust enrichment as an independent cause of action."). Further, some Texas Supreme Court caselaw suggests that plaintiffs may bring claims for unjust enrichment. *See Elledge v. Frieberg-Cooper Water Supply Corp.*, 240 S.W.3d 869, 870–71 (Tex. 2007) ("Unjust enrichment claims are governed by the two-year statute of limitations."). Because Defendants do not conclusively show that Texas does not permit unjust enrichment, they have not demonstrated that Plaintiffs have failed to state a claim on this basis.

Next, Defendants argue that Plaintiffs fail to allege that Mr. Cooper "obtained a benefit from [the plaintiffs] by fraud, duress, or the taking of an undue advantage," as necessary to state a claim for unjust enrichment. Defs.' Mot. 39; *Matter of Connect*

Transp., L.L.C., 825 F. App'x 150, 154 (5th Cir. 2020) (unpub.) (quoting *Sullivan v. Leor Energy, LLC*, 600 F.3d 542, 550 (5th Cir. 2010)); *see Heldenfels Bros. v. City of Corpus Christi*, 832 S.W.2d 39, 41 (Tex. 1992) ("A party may recover under the unjust enrichment theory when one person has obtained a benefit from another by fraud, duress, or the taking of an undue advantage."). Plaintiffs argue that Defendants "diverted funds that should have been used for data security, and . . . unfairly used Plaintiffs' PII for marketing purposes." Pls.' Resp. 38. Plaintiffs fail to connect how the alleged use of Plaintiffs' PII for "marketing and promotional communications," Pls.' Am. Compl. ¶ 518, related in any way to the data breach or that such a purported benefit was obtained by fraud, duress, or taking of an undue advantage.

Plaintiffs' argument that Defendants received an undue benefit through the use of funds they should have used for data security is also unsupported by the factual pleadings. Defendants argue that Plaintiffs "do not allege that *they* paid for data management and security; instead they vaguely allege that Mr. Cooper diverted funds that should have been used for data security." Defs.' Reply 19 (emphasis in original). The Court agrees that the complaint pleads only that "Mr. Cooper funds its data security measures entirely from its general revenue fund," Pls.' Am. Compl. ¶ 513, and does not allege that Plaintiffs ever paid any money to Mr. Cooper for the specific purpose of data security. And because no money was paid for the particular purpose, there is no reasonable interpretation of the facts that plausibly alleges money was obtained fraudulently as though for protection and then used

instead for some advantage to Defendants. Because the Court finds the elements of unjust enrichment are not met, the Court dismisses this claim.

D. The Court Denies the Motion as to the Negligence Per Se Claim

Defendants seek dismissal of Plaintiffs' negligence per se claim (1) for the same reasons that Defendants argue Plaintiffs' negligence claim fails, (2) because the claim is premised on the Gramm-Leach-Bliley Act ("GLBA") and the Federal Trade Commission Act ("FTCA"), which do not constitute negligence per se in Texas.

Unlike the other common law claims, Plaintiffs assert that "the law governing negligence per se varies drastically between states," and therefore the arguments against negligence per se "should be rejected as premature" prior to a fulsome choice-of-law analysis. Pls.' Resp. 36 (quoting *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742 (D.N.J. 2021)). The Court agrees and finds that because a law other than Texas law may apply, and because the law governing negligence per se varies between states, the Court defers judgment on this claim until choice of law analysis is completed at the class certification stage.

E. The Court Grants the Motion as to the Invasion of Privacy Claim

Defendants seek dismissal of Plaintiffs' invasion of privacy claim under the theories that (1) Plaintiffs fail to allege that Mr. Cooper intentionally intruded into Plaintiffs' seclusion, and (2) an invasion of privacy claim cannot survive where the plaintiff voluntarily offered his or her information to the defendant. Defs.' Mot. 41–42. An invasion of privacy claim has two elements: "(1) an intentional intrusion, physically or otherwise, upon another's solitude, seclusion, or private affairs and concerns, which (2)

would be highly offensive to a reasonable person." *Amin v. United Parcel Servs., Inc.*, 66 F.4th 568, 576 (5th Cir. 2023) (quoting *Valenzuela v. Aquino*, 853 S.W.2d 512, 513 (Tex. 1993)).

"There is a split among Texas courts of appeals on whether to recognize a cause of action for negligent invasion of privacy." *Hays*, 2024 WL 4052741, at * 11 (collecting cases). In *Hays*, the court discussed the reasoning of the Texas courts of appeals behind the split and determined that the "Texas Supreme Court is likely to reject a negligent theory of invasion of privacy if faced with such a claim." *Id.* Plaintiffs here cite *Boyles v. Kerr*, 806 S.W.2d 255, 259 (Tex. App. — Texarkana 1991), *rev'd on other grounds*, 855 S.W.2d 593 (Tex. 1993), for the proposition that "an intrusion upon seclusion claim may be premised on either intentional or negligent conduct." Pls.' Resp. 38–39. However, as discussed in *Hays*, the Texas Supreme Court in *Boyle* ruled that the similar claim, infliction of emotional distress, required intentionality rather than just negligence. *Hays*, 2024 WL 4052741, at *11 (citing *Boyles v. Kerr*, 855 S.W.2d 593, 595–97 (Tex. 1993)) ("Had the [negligent invasion of privacy] claim still been part of the case, the Texas Supreme Court would have been likely to reject the claim based on the same reasoning."). The Southern District of Texas has adopted similar reasoning in *Logan*. 2024 WL 3489208, at *9 ("Because invasion of privacy is an intentional tort, a theory based on negligent failure to safeguard and protect personal information is insufficient to state a claim for invasion of privacy." (cleaned up)).

Plaintiffs here also cite to *Smith*, 747 F. Supp. 3d 989, to show that Texas courts have sustained invasion of privacy claims in the data breach context. Pls.' Resp. 39 n.16.

The *Smith* court concluded that the plaintiffs stated a plausible claim for intrusion upon seclusion but did not undertake any analysis. *Smith*, 747 F. Supp. 3d at 1003. The Court therefore finds the detailed analysis from *Hays* and *Logan* more persuasive and dismisses the claim because Plaintiffs fail to allege that Defendants intentionally invaded their privacy.

F. The Court Grants the Motion as to the Breach of Confidence Claim

Defendants move to dismiss Plaintiffs' breach of confidence claim because breach of confidence claims are limited to the trade secrets context. Defs.' Mot. 42–43. This Court has previously found that "a breach of confidence claim mirrors a misappropriation of trade secrets claim." *Richter v. Carnival Corp.*, 2019 WL 5894213, at *7 (N.D. Tex. 2019) (Godbey, J.) (citing *Hyde Corp. v. Huffines*, 314 S.W.2d 763, 769 (Tex. 1958)). Plaintiffs have not provided authority, nor is this Court aware of any authority for a reinterpretation of breach of confidence beyond the trade secrets context to include any information that may be kept confidential. *See Logan*, 2024 WL 3489208, at *11 (finding no authority for a breach of confidence claim under Texas law). The Court, therefore, declines to reinterpret breach of confidence outside of the trade secrets context and grants the motion to dismiss this claim.

V. THE COURT DEFERS JUDGMENT ON STATE CLAIMS

Plaintiffs bring nineteen claims under a variety of state laws, which Defendants now move to individually dismiss for failure to state a claim. The Court finds that class certification is a logical antecedent to the analysis of the individual state claims that derive

from the subclasses within the larger class. Therefore, the Court defers judgment on Claims IX–XXVII until the class certification stage.

CONCLUSION

Because the Court finds that Plaintiffs have standing, the Court denies the motion to dismiss as to Defendants' standing argument. However, the Court finds Plaintiffs' claims for declaratory and injunctive relief too speculative and does not find standing for those claims. Then, the Court finds that Plaintiffs have alleged sufficient facts to state a claim for their breach of implied contract and negligence claims and denies the motion to dismiss as to those claims. Next, the Court finds that Plaintiffs have not alleged facts sufficient to state a claim for breach of express contract, unjust enrichment, or invasion of privacy and grants the motion as to those claims. Because Plaintiffs did not seek leave to amend pleadings for these claims, and the Court finds that amendment would be futile, the Court dismisses these claims with prejudice. Finally, the Court defers judgment on the negligence per se and state law claims until the class certification stage.

Signed July 22, 2025.

David C. Godbey
Chief United States District Judge